

DRAFT SDC PCPP Private Cloud Requirements DRAFT

Agency Q&A during Workshops

Migration and System Integration Issues Resulting from Standardization

1. In what service model does the software version and level of standardization become a hindering restraint in moving into the proposed use cases?
A It applies to all (IaaS, PaaS, SaaS) at some level, but IaaS is the least restrictive.
2. How will custom middleware be handled (i.e. we have 40 databases on a single SQL server) in the new environment?
A For such instances where the requirements are too complex to move into the use case 1 (“utility”) environment we will utilize use case 2 (“secure multi-tenant”).
3. How do you define middleware?
A Middleware is comprised of application and web servers. The State’s current portfolio and what runs in it will drive the solution used and whether the Cloud Supplier can manage it.
4. We currently have a failover system which minimizes service disruption; can we continue this in the Cloud Environment?
A That will need to be addressed, but these are the kind of requirements we are looking to capture so they can be applied to the solution.
5. Will standardizing the cloud platforms make it easier to move to a different Cloud Supplier or overall solution?
A Yes, this is part of the mitigation of execution risk. Making it more portable and getting applications into this environment creates more options for the future and will reduce costs associated with expensive ‘one-offs.’
6. Will there be changes made to firewall configurations? If the HRMS firewall is altered, the system will no longer function? It has yet to be virtualized at this point.
A Only virtualized systems are in scope for this project. The details of the SDC firewall are not yet established, but HRMS will be receiving special attention.

7. Will this cloud environment utilize a single hypervisor solution and is it possible to have multiple?
- A** We are recommending standardizing on a common hypervisor solution because multiple solutions will drive costs up.

Disaster Recovery

8. For the Disaster Recovery solution, will it be onsite in the SDC or elsewhere?
- A** Both inside and outside of the SDC solutions will be explored. We will ask for the Cloud Suppliers recommendation but ultimately, the solution must be cost effective.
9. Will the Disaster Recovery site be cold or warm? Will there be excess capacity?
- A** The Cloud Supplier will be required to propose Disaster Recovery as an optional service. Because it can be very expensive, it will likely become a financial decision on what solution is used.
10. If I go to provision or procure a server, will I be able to select Disaster Recover as an option (i.e. Prod vs. Pre-prod servers)?
- A** This option as well as the underlying functionality will need to be explored further with the Cloud Supplier.
11. How many infrastructure environments use a cloud solution for Disaster Recovery?
- A** At this point, the percentage is unknown, but this method is gaining in popularity and trending upwards.

Compliance and Security Uncertainty

12. Does legal liability for the data pass to the service provider because the cloud environment is being provided as a service? Are the agencies released of this responsibility?
- A** CTS and the Customer Agencies are still responsible for the data, but we are very well positioned to mitigate any risks because the private cloud will be contained in the SDC.
13. Is the reason for having a separate set of infrastructure connected to public internet driven by an ISB or compliance standard?

- A** Not necessarily, ISB is primarily concerned with how the service will be performed; this is one of our architectural requirements. SDC requirements have separate environments for external facing equipment. Currently, our external environments are non-proxy access, so it needs to be continued in the new environment.

14. Will there be compliance standards for security products?

- A** Absolutely, we will thoroughly review security and compliance requirements. There will be a set of appendices that contain all requirements which will then be referenced and woven into the RFP documents.

15. Are the Cloud Suppliers aware of our required security compliance standards and will it be a standardized solution?

- A** There is a great deal of work being done with the IRS, who is publishing work on how these suppliers can be compliant. For the workloads which require more rigorous security compliance, it will be provided, but there will need to be working sessions with the Cloud Supplier to determine the specifics of how/ if different levels of security will be possible within the same physical boxes.

16. Will this solution comply with ISB security standards?

- A** Yes, this is included in the RFP requirements.

Procurement Process and Provisioning Tools/Functions

17. How will provisioning work for the two use cases?

- A** The expectation for use case 1 is to utilize a web based portal, provided through a Cloud Supplier's web based service catalog. For use case 2, it will need to be researched, but it may go through a change management process of notifying the Cloud Supplier. UPDATE: Use case 2 will also use a web based portal.

License Ownership and Concern for Stranded Assets

18. How will licensing be handled on a virtual machine with multiple cores?

- A** The Cloud Supplier will be responsible for acquiring licenses and ensuring compliance with all licensing terms for virtual infrastructure software in both use

case 1 and use case 2. The Cloud Supplier is also responsible for licensing operating system, database, and middleware software in use case 1. For State of Washington owned software, we will need to contact vendors to ensure compliance when transitioned into a virtual/cloud environment.

19. Are we going to walk away from all of our current State of Washington Owned Licenses?

- A** Once a transition to a use case 1 environment is complete, they will become stranded costs. However, as the transition occurs, there will be a savings in maintenance fees.

Cloud Supplier Owned Infrastructure Concerns

20. Can the State of Washington retain ownership of the environment at the end of the contract?

- A** An option to purchase may be available through the contract language, but there are special considerations that may make this impossible for state government.

21. What if the Cloud Supplier goes out of business or is unable to perform the required service? What if the Cloud Supplier cannot or does not meet the requirements?

- A** We need to be very careful to weed out unqualified Cloud Suppliers and select only those with sufficient commercial viability.

22. What is meant by level of commitment as it pertains to the different service platforms the Cloud Supplier will be providing?

- A** The level of commitment is the length of time you are contracted with a particular cloud supplier. As the service being procured moves up the stack (IaaS>>PaaS>>SaaS), the level of commitment decreases.

23. How many contracts are signed with a different Cloud Supplier after the first five years, second five years, 3rd five years? Should we expect a 50/50 chance to switch Cloud Suppliers after five years?

- A** It is entirely dependent on performance, but this customer-supplier relationship will be much closer than normal instances because the Cloud Supplier will have their assets in the SDC.

Delineation of Roles within Release Management

24. Why is the Cloud Supplier to be responsible for Change Management but not Release Management?

A The Cloud Supplier will assist in Release Management, but will not own this responsibility because the State of Washington will be retaining responsibility for applications.

25. What role will the agencies play in ensuring the Cloud Supplier compliance? Do we need to perform our own compliance audits? Shouldn't CTS be responsible for this if they are supplying the platform? How will this be handled for small agencies that do not have vast resources?

A CTS will manage the performance of the Cloud Supplier, but ultimately the State of Washington owns the results. The RFP requirements will include responsibility for the Cloud Supplier to perform their own compliance audits and service levels will also be defined in a way to ensure necessary focus on areas of concern. There will also be an ongoing contract management process owned by CTS which will hold the Cloud Supplier accountable for performance. CTS Mainframe service is currently set up in this manner and CTS owns the responsibility for the results.

26. How will the agencies move applications between environments and handle release management?

A Promoting or backing out applications will be supported by the Cloud Supplier, but not controlled by them.

Collaboration on Planning

27. Is the Cloud Supplier responsible for performing capacity management?

A Yes.

28. What if the Cloud Supplier changes the cloud technology or cloud configuration and it breaks my application?

A They will be obligated to make Customer Agencies aware of any changes and will be responsible for all related communication.

29. How do we ensure the Cloud Supplier is an active participant in moving our technology forward and making sure our final solution will have good longevity?

A This will be a component of the required dialogue with the Cloud Suppliers and a part of the contract management requirements, to be governed by CTS.

Pricing Cost

30. Will pricing be based on utilization? Will it be fixed? A combination?

- A** The concept to be deployed is to pay for what you're using; the pricing and cost model has yet to be developed.

Scope

31. Is the target of this new service to go beyond state agencies?

- A** Yes. CTS is buying a private cloud environment to provide to the customer agencies, but it is a dedicated environment to CTS. This enables us to eventually provide service to cities, counties and non-profit organizations, within the scope of the legislation.

32. Is it possible to give preference to those who are looking for PaaS? We can virtualize level 2, but level 1 is very tough and will require redevelopment.

- A** These requirements will be integrated into planning.

33. Why is PaaS not being offered as a possible use case?

- A** Enterprise grade PaaS is not yet available in a capacity which can sufficiently support the SDC.

General Comments/Remarks

34. Is it common practice to have an external Cloud Supplier providing this service within the confines of a customer owned datacenter (the SDC) and will we get a lot of bids?

- A** There are currently instances of this happening, but each instance is different and has its own set of unique challenges. We need to carefully integrate our requirements in a manner which will attract a variety of Cloud Suppliers to bid.

35. Will we be solicited for information?

- A** Yes, data collection will be very important to building an RFP that both provides us excellent service and is attractive to bidders.

36. What is the current market share breakdown between PaaS and IaaS?

A Current 5 year projection is split 90% - SaaS and 10% - IaaS+PaaS.

37. We need to have a good reverse transition plan (transition assistance) for each aspect:
Skilled labor, purchasing hardware, licensing, etc.

A Acknowledged and agreed

38. If we move to a new system in a couple years, need to make sure the transition is well executed and troubleshooting of any issues is a Cloud Supplier responsibility.

A Acknowledged and agreed

39. Must be collaboration on planning for capacity, architecture, application deployment, etc.

A Acknowledged and agreed

40. The Customer Agencies are surprised that The State of Washington owning the infrastructure is not being considered.

A It's CTS's intent to offer a co-managed service which allows control and visibility by customer agencies.

Service Levels – General Discussion

41. Is there consideration for duration and frequency of missed service levels?

A In general, yes. It depends on how the service level is defined, but this can certainly be accommodated

42. Is the service level credit the same for each occurrence of the same event? Is there an incentive to avoid repeat offenses? Does the credited amount go up?

A The credit is not increased with frequency because the Cloud Supplier will not agree to this. Such an agreement would force the Cloud Supplier to raise their price to cover the associated risk. The best course of action for the State of Washington is to increase the % of the 'at risk amount' for certain things if there continue to be service level defaults.

43. Is the service level credit calculated based on duration of the 'outage' or named violations?

A The credit is a pre-calculated amount based on whether or not the service levels are met, they do not fluctuate with the duration of the event unless specifically

written to do so.

44. Do service level measurements restart after a certain time period? Are they measured on a rolling period?

A Some service levels will be evaluated on a rolling 12 month period.

45. How will infrastructure service levels be measured?

A It will be measured at the perimeter. If the infrastructure is down in a way that it affects our operations, then the appropriate credits will be calculated and applied.

46. Given the discussion about platform compatibility, should we also consider going in the other direction (moving from cloud to non-cloud)?

A There are occasions where this can happen, but they should be rare. For example a current application that evolves into a legacy application may, over time, no longer be a candidate for cloud.

47. Will the state of Washington be utilizing the Cloud Supplier's enterprise agreement for the licensing?

A The Cloud Supplier will be responsible for acquiring and ensuring compliance of Licenses for all virtual infrastructure software and use case 1 platform software.

48. For those of us with large enterprise licensing agreements, will anything be done to incentivize us to transition?

A Timing will be a large factor, but incentive hasn't been discussed as of yet. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

49. When does the service level 'clock start' in the event of an incident? How does additional time come into play if we have to escalate to CTS and CTS to the Cloud Supplier?

A The clock starts when the Cloud Supplier becomes aware of the issue, either through their monitoring tools, or from notification by CTS. We need to consider what data is available for the Cloud Supplier to be measured against, so the starting point is when they are notified/when they become aware.

50. Is 4 hours time to repair reasonable, how does this translate into an end to end service level?

- A** The industry recognizes 4 hours as reasonable and current CTS vendor agreements dictate 4 hours.

51. Is there a ceiling of how many provisioning requests the Cloud Supplier can expect in a given time period?

- A** This will be part of the data collection effort. As we learn about the number of applications and hardware, we will get closer to a reasonable estimate for adoption of both use cases and how many requests that will translate to.

52. How will new software/hardware and advancements in technology be handled?

- A** The State of Washington is buying experience, expertise, innovation, research and development, and technical currency. It will be expected that the Cloud Supplier is responsible for keeping the environment up to date and supporting new technology as will be defined. For example, we will create a mandatory requirement for the cloud supplier to support an O/S or Database as long as the original vendor supports it. We will also create requirements that the cloud supplier must support a new version of a supported OS or Database within a reasonable time, TBD.

53. How long will they support older versions?

- A** It's not desirable for a supplier to be able to force you off your application and discontinue software support. For now they will not be allowed to discontinue support for any older versions. We will enforce this by creating a mandatory requirement that as long as the supported OS or database is supported by the vendor, the cloud supplier must support it as well.

54. If a capacity incident occurs every month, can we redefine these specific requirements mid-contract? Who would ultimately make the decision to implement a change?

- A** Yes, but we need to be careful not to overcomplicate the service levels. What we can do is raise the weighted % of certain service level to increase the credit and draw the Cloud Supplier management's attention to these issues.
- A** CTS would implement with input from the Customer Agencies, but for capacity they will not agree to as stringent of service levels because it's deployed in the SDC.

Service Levels – Scope

55. What is measured and constrained by the Capacity Management service level? Does this mean capacity management regarding bandwidth, CPU resources, storage? One incident per quarter seems excessive.

A An incident stemming from any of those shortages would trigger a service level credit. We will examine the frequency, but planning will be important to ensure available capacity.

56. For Use Case 2, will the Customer Agencies be standing up their own servers and loading their preferred OS?

A For use case 2, the solution will be to use the Cloud Supplier's tools to provision hardware and the hypervisor. The Customer Agencies install their own OS, software, and applications.

57. For Use Case 2, if the Customer Agency is to install the guest, why will it take 3 days for them to stand up the server?

A It should not require 3 days. TPI has seen several recent IaaS contracts where manual intervention is required on behalf of the cloud supplier. However, based on customer agency feedback, and based on additional research, TPI is recommending that the State require the cloud supplier to have automated provisioning for both use cases, therefore, there will be only one service level reflecting this

58. Does there need to be a Use Case 3 developed for Co-location? - The Cloud Supplier has no role except for provisioning hardware?

A Co-location is outside the scope of this procurement. There may be instances where co-location is necessary, but that will be determined through our data collection process. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

59. How will the SLAs apply to development/test environments?

A There will not likely be any different or unique SLAs associated with development/test environments. The existing set of SLA's will apply to those as well.

60. What about failover and availability? If one of my servers fails now, it is immediately supported by a failover server; will this service exist through the Cloud Supplier?

A We will look into this requirement.

61. Will load balancing be included as a template or a service?

A Load balancing services are included and the specific requirements are coming from the shared services group.

62. Is the scope of the data collection for Thurston County or State wide?

A Thurston Country, but this will be clearly defined on the distributed template.

63. What if there aren't offerings for the services we require?

A This is an important part of early planning to ensure as much service can be provided as possible. The intent is to leverage the new environment to improve service and reduce costs. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

64. Can we have our own dedicated network for a particular application? Could that application be hosted in this environment?

A There will be a separate infrastructure hosted on the PGN that may be able to entertain this, but will likely be evaluated on a case by case basis. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

65. Are SGN and PGN instances part of the RFP?

A Yes and it is a requirement for them to be separate, but the Cloud Supplier will tell us how they will execute this and how much it will cost.

66. Are these service levels inclusive of Disaster Recovery?

A Disaster recovery will be bid as an optional off-site service. As the DR infrastructure will not be in the SDC, the same infrastructure service levels will not apply, but service levels specific to DR will be developed.

Service Levels – Vendor Management

67. Will it be mandatory for the Cloud Supplier to supply a measurement tool/visibility for agencies? Do they need to provide us with a mechanism for us to verify the status of the environment?

- A** Yes, we are requiring the cloud supplier to provide the state visibility into the usage and performance of the cloud platform.
- A** Cloud Suppliers will provide the backup data and hard statistics/measurements which will allow for their reports to be audited.
- A** There will be a State of Washington vendor management team responsible for monitoring the infrastructure availability and any due credits.

68. Why can't the State of Washington dictate cloud supplier scheduled maintenance?

- A** Both parties will need to actively participate in planning, but more than likely, the supplier will not agree to mandated maintenance schedules. However, based on customer agency feedback in workshop #2, TPI is recommending a strong position on this subject, whereby maintenance will be scheduled and approved by State during mutually agreed time frames

69. If there are several incidents, how can Customer Agencies pick which issue receives immediate attention?

- A** These issues are not managed through the service level methodology, but will be part of the vendor management structure. CTS will be responsible for service delivery and conveying special needs/prioritization to the Cloud Supplier. CTS will ultimately be responsible for determining incident priority level, not the cloud supplier.

70. Will it be possible to escalate issues? How will that be established?

- A** Absolutely, CTS will be the interface who will escalate to the Cloud Supplier. There will be a defined workflow for the escalation process. There will also be a great deal of reporting and process discipline which will empower CTS to provide the desired information to Customer Agencies.
- A** It is the intent for customer agency to interface with CTS as occurs today.

71. Regarding the algorithm for calculating credits; who will notify who in the case that an application is down? Does the Customer Agency have to open a ticket with CTS or is the service provider informing us of the outage?

- A** Both scenarios will exist. If the cloud supplier becomes aware first, they need to enter it into their system and notify the appropriate State of Washington personnel. If the end user finds an issue first, then they will bring it to the attention of CTS and if CTS can't resolve the issue, then it will be escalated to the Cloud

Supplier. Until it gets to the Cloud Supplier, they can't track it as an incident, so if they do not discover the incident first, they will become involved via Service Desk Level 3.

72. If an outage occurs, does the Cloud Supplier monitor the event and notify the customer?

A Absolutely, they will monitor and enter a ticket. For notification, the cloud supplier will have to write an operating procedures manual for the escalation path to the authorized user.

73. We need to require notification at intervals as problems are diagnosed and resolved. Can Customer Agencies receive status reports during the resolution process? Receiving confirmation that the problem is solved is important, but we need periodic updates.

A We will ensure status updates are a requirements.

74. What about the Service Level relationship between the Customer Agencies and CTS?

Customer Agencies need a strong relationship/agreement to ensure these service levels filter down to the Agencies, not just CTS.

A Absolutely, there will need to be a SLA between CTS and the customer agencies. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

75. Can we prioritize systems? There are certain systems the State of Washington cannot afford to be without (i.e. payroll/unemployment).

A This will happen through operational communication and delivery management systems.

76. Are measurement windows ever restarted? We do not want them to reduce priority if they know they've already defaulted on a particular service level.

A The best tool is that we can change the % associated with each service level for the following month.

A Rebecca needs specific business process issues from the Customer Agencies as soon as possible.

77. It appears this is no longer a relationship but an SLA. Do we need to define every line and protect ourselves?

- A** The service level methodology is a tool to force the management's attention to highly prioritized issues, but the real work is in the relationship management.
- A** The foundation of vendor management will be a very important focus of the Cloud Supplier.

Service Levels – Backup / Storage

78. Is the Cloud Supplier responsible for backup and storage?

- A** Yes, and these will be explicitly defined within the RFP

79. If you're backup was successful, why wouldn't the restore be good as well?

- A** Cloud Suppliers will argue that matching restore and backup rates is very unlikely to occur at 100%.

80. Are the backups being performed pre-defined by the Customer Agencies?

- A** We will be requiring the cloud supplier to 1) provide backup services as part of the standard offering and 2) requiring the capability for customer agencies to perform ad hoc backup/snapshots as needed.

81. How long will the supplier retain backup data?

- A** Aaron has defined this in current security standards, but we will need to make sure it aligns with all other contract language.

82. For storage, do we know the specific rate configuration and spindle?

- A** This will be asked of the Cloud Supplier and they will have to explain how they will handle it.

83. In use case 1, will tiered storage be an option?

- A** Absolutely.

System Requirements

84. How will we ensure the integrity of their monitoring tools as they will be using these to do root cause analysis?

- A** Part of the RFP will demand the bidder inform us of how they will gather this information so we can ensure it is credible.

85. What level of support will be provided for BizTalk?

- A** Through the data collection process, we'll determine what, if any, middleware should be included in Use Case #1. The level of support will depend on the application; however, it will follow the same model as O/S and Database.

86. Will Customer Agencies receive a SQL database as a service or as a server?

- A** SQL databases will be provided as a service.

87. As the Customer Agency, will I be able to deploy as many databases as I want on these provisioned servers?

- A** Yes

88. Will clustering be an available option?

- A** A strong demand has not been expressed thus far, so if there is a strong enough demand, we need to be notified immediately.
- A** In workshop #3 it is clear that there may be a stronger demand for this, so this will be added as a desirable requirement.

89. Will everything be duplicated in a development environment and will Customer Agencies be able to select which environment we need?

- A** Yes to the second part of the question. To the first part, a development environment will be provisioned through the same process, and using the same infrastructure, as a production environment.

90. Will there be the ability to change your provisioned environment over time?

- A** Absolutely.

91. For use case 1, can you stop somewhere up the stack (i.e. middleware) and install our own SQL servers?

- A** It is possible, but TPI does not recommend this approach, given that we are asking the cloud supplier to provide a managed database service in Use Case #1. In this instance, Use Case #2 is a better candidate.

92. Will Customer Agencies be able to install database servers on a Use Case 1 provisioned server? Will this create licensing issues? Will Service levels be compromised for devices with this 'custom' configuration?

A TBD

93. What if there is a custom application that will not function within the standard set of OS?

A If some requirements become too unique, the application will have to move to Use Case 2.

94. Can there be multiple and customizable patch windows?

A This is yet to be determined, but it is difficult to dictate maintenance windows to the Cloud Supplier and could create an issue for them. However, we will be making it a requirement that the Cloud Supplier maintenance to be scheduled and approved by State during mutually agreed time frames

95. Will there be segmentation for compliance purposes?

A Yes, this is spelled out in IT security standards and external standards that are being leveraged.

96. Will we have restrictions on using hardware based appliances?

A It will depend on where it is located, if needs to be located inside the Cloud Suppliers managed area, they will not want any equipment in there they cannot control.

97. Could we use appliances that are located outside the cloud on our network segment?

A That will be driven by security requirements.

98. Can we determine isolated requirements?

A The Cloud Supplier will tell us how they will provide it and how it will be executed to be security compliant.

99. Is there uniqueness and division between the agency environments?

A The intent is CTS will provide Vlans and IPs for all customers to make sure routing occurs correctly across the datacenter so that logical separation is in place.

100. Will the Customer Agencies have admin access on the servers in Use Case 1?

- A** Customer Agencies will definitely need the ability to build and deploy as needed, but the Cloud Supplier will need to participate in how this will occur. In workshop #3, we clarified this position to make sure it was clear that the cloud supplier will be the admin in use case #1.
101. Will the Cloud Supplier be able to accommodate custom software configurations with custom back up requirements?
- A** The specifics will dictate if this will be possible, we'll have to address with the Cloud Supplier.
102. Can we expect any changes to current Active Directory configuration, as this has large implications?
- A** Active Directory requirements are still being developed at this time.
103. Will Customer Agency development efforts be transfer into the cloud environment?
- A** Yes, the Customer Agencies will realize one of the benefits of a cloud environment here. It will be possible to provision a box for a few weeks and then spin it down when it's no longer needed.
104. Customer Agencies need to be provided visibility/information on how applications are performing, how will this be delivered?
- A** We will need to determine whose set of monitoring tools will be utilized to do this (State of Washington or Cloud Supplier). From there, we can dictate what performance information is required. This is an issue that CTS owns, and will not need to be addressed as part of the RFP for the Cloud Supplier.

Service Level - Definitions

105. What is the definition of 'Infrastructure Uptime?' Does this mean one small piece of the environment or the datacenter core? What happens if it's a cloud problem or a network problem? Customer Agencies are not concerned where the problem lies, but that it is corrected quickly.
- A** A document of all of these terms and definition is being developed.
- A** Demarcation points are being finalized and whichever side the problem lies on, the responsible party will apply the required solution.

106. What does 'resolve' mean? Does this mean a work around is developed or an actual solution?
- A** This will mean that service is restored to a level that meets the expectations of the contract.
107. How are the 'urgent' and 'high severity' levels determined?
- A** Similar Cloud Supplier contracts are being examined to find the optimal balance so that they are stringent enough to demand a high level of service, but not too tight that bidders are scared away.
- A** These have since been drafted via an industry standard framework that has been tailored to the State's requirements and presented in the next workshop.
108. For the data collection, are we counting cores or physical CPUs?
- A** Physical servers will be counted by cores and virtual instances counted by CPU, this will be explained in the collection template.

Pricing Construct

109. Is it possible to have transparency into the financial build of all infrastructure pricing components? This would be very helpful for Customer Agency forecasting and help better managed costs.
- A** This is precisely the detail that CTS is requiring of the Cloud Supplier, but we will not be able to see actual supplier costs.
110. If the pricing model shows decreasing rates in later years, how will CTS ensure the early adopters are not being penalized?
- A** Similar to how the cost offerings for the Secure Email project were managed, CTS will likely adjust the pricing that is realized by the Customer Agencies. This would have CTS taking an initial loss in the beginning of the contract and making it back on the back end. The specifics have not been finalized, but whatever the solution, it is our intent to prevent early adopters from being penalized.
111. How is the commitment to these new Use Cases being determined? The survey did not ask which use case we'd like to adopt or when we'd be able to move.

- A** We don't need to know the adoption between Use Case 1 and Use Case 2 because we don't expect a drastic difference in the Use Case pricing. The commitment levels as a whole and timing will need to be examined and discussed.
- A** CTS and OCIO will be reaching out to each agency to see if there is any initial volume that can be committed to the initial move.

112. What if we do not move very much volume in until the end?

A TBD

113. Are we going to be asked for an adoption commitment once the use cases are finalized?

A Yes, CTS and OCIO will be reaching out to each agency to discuss levels of commitment as well as transition planning.

Resource Units

114. Will thin provisioning be used for the utilization based pricing model?

A That is the intention, we will confirm to make sure this is not misinterpreted.

115. Will the cost be adjusted for agencies that resell these services?

A This will need to be analyzed side by side once pricing is submitted from the suppliers.

116. Is the DR offering intended to be a single, one size fits all option? There are many different configurations that should be considered.

A DR is a very high priority and all options are being explored.

117. It was mentioned that the DR would be hosted to an offsite, possibly Cloud Supplier data center, if this is the case, would I be able to set up my own DR that maps back to my facility?

A Potentially, but DR requirements and configuration is still being worked through.

118. How will you decide on the Disaster Requirements?

A Many of the requirements will be driven by the Shared Services Group pre-existing needs, but this will be sorted out shortly.

119. Will Customer Agencies have the ability to implement DR on an application by application basis?

- A** This was the initial intent, but led to the realization that it may overly complicate things so we need to examine the varying scenarios for DR and how to go about asking for this within the RFP.

120. Beyond DR, what about backup and restore, will this also fit into this DR model?

- A** Yes, of the 3 storage tiers, our high level recommendation is that the backup would be included in the storage tiers.

SLA – Priority Level Recommendations

121. Will there be a mechanism to override certain service levels or escalate them to a more critical level?

- A** Yes, the State of Washington will have absolute authority to direct the Cloud Supplier to respond at a desired priority level.

122. Will there be service levels associated with these priority levels?

- A** These will not be critical service levels, but key measurements. The key measurements are monitored and can be escalated to have ‘at-risk money’ tied to them if needed.

123. Could ‘members of the public’ and ‘public safety impacted’ be metrics used to drive a priority level?

- A** Yes, we will incorporate these into the definitions. Furthermore, there will be a required operating manual built by the Cloud Supplier and approved by the State where the specifics will be spelled out.

Adjustments to Service Level Matrix

124. Could you expand on what ‘down-time’ consists of? Is it interruption of an application? A subsystem being down?

- A** When any piece of the services/infrastructure goes down in such a way that the State of Washington is impacted.
- The *application* wouldn’t trigger a default in the service level as it will be out of the Cloud Suppliers scope.

125. Shouldn't there be zero hard down time, as there are no maintenance windows that accommodate all agencies?

A It's always been a challenge as State business has varying required uptimes. We will figure out how to position this, but it's a problem we face even in the current environment.

126. Would a 'hot' failover option be possible for one of the DR solutions?

A That will be considered.

127. How can we mitigate finger pointing for cause of incidents in use case 1? Won't the tight linkage between application and the infrastructure create issues in determining root cause?

A Yes, this is a very difficult issue to mitigate; this will require that application testing is very thorough before promoting to production.

128. Has GMAP reporting been taken into consideration? How will we get the required reporting metrics for each incident?

A CTS will need the specific measurements that are needed by the Customer Agencies, but it is required in the RFP that all needed metrics will be tracked by the Cloud Supplier. CTS will likely hold the responsibility for this information and its distribution.

129. Will we need to call CTS/help desk to get the necessary reporting details? Can the agencies get this information directly?

A This relationship will be between CTS and Agencies to figure out. CTS will ultimately need to provide it.

130. Will provisioning services be provided 24x7?

A Yes, that is the expectation.

131. How will the cost of databases, OF, Software support be paid?

A All support of the environment is built into the unit rates.

132. Won't use case 1 become a landing pad for servers that require very little maintenance and work in current state?

A Yes, it should be a less demanding environment to manage.

133. How will pre-built machine images be accommodated?
- A** There will need to be a list for use case 2 of operating systems that will run on this version of the hypervisor platform.
134. If they are going to perform infrastructure upgrades, how do we test to ensure our applications will still function properly?
- A** The Cloud Supplier will have to provide advanced notice and coordinate with CTS to ensure there are no issues before applying any changes.
135. What is a reasonable time period to expect the Cloud Supplier to provide new service packs and new software?
- A** Three to six months.
136. Has any thought been given to allow use case 2 to be provisioned by CTS instead of pushing it out to supplier? Couldn't we then use our own licenses?
- A** It has been considered, but there is a great deal of complications aside from licensing (e.g. we would still need to change our licensing to "service provider" class)
- A** Cloud suppliers wouldn't be able to configure our servers once they are provisioned.
137. In the middleware layer, many organizations do a lot of fine tuning. Will there be any way to rapidly provision this customized configuration?
- A** Great observation, please note this requirement in your data collection template and we will look into it.
138. Can you describe the backup and recovery scenario for the use cases?
- A** We are making it a requirement that it must occur for both use cases, the Cloud Supplier will have to provide details behind their proposed solution(s).
139. For use case one, isn't it back up method determined by the Cloud Supplier?
- A** Yes, but we will dictate our access to those backups, how often and in what manner. We are still working out requirements (difference between back up and archive).

Pricing Tiers/ Storage

140. It appears the storage tiers are not based on performance; can this be built into the model as well as established storage response times?

A Yes, we will factor that in, but ultimately, the Cloud Supplier will propose storage solutions for the State of Washington to approve based on defined needs.

141. Is Tier 3 storage a category for less critical items?

A Yes.

142. Will test and development storage be captured within these 3 -5 tiers?

A Yes, these tiers will be available for use for all environments (prod/pre-prod/dev/test).

143. Will they have to respond with specific storage measurements?

A That is a good point and we will have to look into this.

144. Can I have a pair of clustered servers in these environments?

A This will be researched.

145. Will we have the ability to create an image and reproduce it on a needed basis?

A This will be researched.

146. Will hardware load balancing be provided by the Cloud Supplier?

A Yes, this has already been included in the RFP.

147. Can I spin up a new VMware image in either use case due to performance spikes?

A This will be researched.

148. Will 10G network/infrastructure be a requirement?

A Yes, the trunk line will be handed to the Cloud Supplier; their infrastructure will be required to support it.

149. Should we solicit feedback from the application development personnel to ensure we examine these use cases from all angles?

A Yes, that's a great idea and we'll explore soliciting more feedback.

150. Will there be a link from the cloud to the co-lo environment?

A There will be connectivity into other state data center offerings within the SDC, but the issues are still being examined.

151. How will the connectivity affect CTS current offerings, especially security gateways?
A All the functionality will still exist, but specifics still being discussed.
152. Will the trunk be layer 2 or 3?
A Layer 3 will have to exist within the cloud, the requirements outside of that are still being established.
153. Could the layer 2 be extended into my Customer Agency datacenters so we could do consolidation and conversation?
A This will be researched.
154. Will Customer Agencies be able to operate a Business Objects environment in Agency datacenters and the cloud or is it simply one or the other? At some point we'll likely have items that exist in both sets of infrastructure.
A This will be researched.